ABSTRACT OF THE DISCLOSURE

An approach for arriving at a shared secret key in a multicast or broadcast group environment is disclosed. The key exchange protocol permits nodes within a multicast or broadcast group to compute a shared secret key in a binary fashion, whereby a shared secret key is generated for a pair of nodes at a time. Once the shared secret key is computed by the pair, the nodes within the pair is viewed as a single entity by a node that is to be joined. This process is iteratively performed until all the nodes within the multicast group attain a common shared secret key. Under this approach, the number of messages exchanged between the nodes for establishing the secured channel is significantly reduced.